

Forum:[Hack Forums](#)

Thread: [Question about MITM on LAN with regard to SSL and Certificates](#)

am0rph0us - February 9, 2023, 9:36 am

I want to learn how to effectively do MITM attacks and sniff traffic on a wireless network.

I've tried to use ettercap and arp spoofing which is the old traditional way of doing it. The problem is that SSL and certificate pinning causes basically every site to say "Certificate not valid" or something like that and it will not even give you the option to proceed. Same thing if you successfully launch a DHCP spoof. Even without using an SSL strip. The main goal is not even to intercept credentials, but to just see the websites being visited and browser version, etc.

What I don't understand is how the problem arises as soon as I set my computer between the target and the gateway. There must be a way to seamlessly flow the data through the attacking machine without causing interruptions and certificate errors.

I have a second option though. I have access to the router admin panel, and since all traffic flows through the gateway I should be able to use this to monitor the traffic.

The router allows me to set routing rules for the network. So I can enable static routes in the format:

Network/Host IP | Netmask | Gateway | Metric | Interface | ADD/DELETE

So here I guess I could set the target IP as the Host IP, then my attacking machine as the Gateway?

Are there any good tutorials on how to set up a MITM attack through the router panel, and would this work?

In general, are MITM attacks even a threat these days with HSTS and certificate pinning? Seems like there is no way to get access to credentials or in my case see the traffic even though I'm on the same WiFi. Driftnet and other tools could be used aswell to see what is being sent through the wires.

Are there ways you could get access to other systems on LAN using some sort of social engineering attack? I want to try to see if I can use DNS spoofing and Beef and get that to work. I've heard there are ways to inject files through the traffic in certain ways.

Any help and links related to this would be appreciated. I know mitm attacks used to be a thing a few years ago, but I would like to hear if anyone has more recent knowledge on Mitm attacks. And if my router approach is viable.

DramaKing - February 9, 2023, 10:08 am

That's funny because I haven't encountered SSL breaking with bettercap (don't use the old version). ARP spoofing works at a lower layer and shouldn't interfere with certificates. However, if you try to set static routes that way, you could break routing. Host IP is the destination, and Gateway is the IP to send packets to for routing to the host. It might sound like it should route all traffic destined for the host to your machine, but we are talking about routing. I have no idea what would happen if you tried this within an internal network.

Have you considered switching to bettercap and using the hstshijack caplet?

am0rph0us - February 9, 2023, 11:43 am

(Feb 9, 2023 11:08 AM)DramaKing Wrote: [\[CITE\]](#) That's funny because I haven't encountered SSL breaking with bettercap (don't use the old version). ARP spoofing works at a lower layer and shouldn't interfere with certificates. However, if you try to set static routes that way, you could break routing. Host IP is the destination, and Gateway is the IP to send packets to for routing to the host. It might sound like it should route all traffic destined for the host to your machine, but we are talking about routing. I have no idea what would happen if you tried this within an internal network.

Have you considered switching to bettercap and using the hstshijack caplet?

Yeah that's what I thought as well, spoofing in layer 2 should not interfere with layer 5 but somehow when I use ettercap arp spoof it breaks. Arp spoofing "manually" with forwarding and ip tables doesn't intercept anything at all, maybe im doing something wrong or something in my setup is broken.

Thank you for the suggestion though I will try to run bettercap instead and see if that works.

----- Edit

Bettercap worked nicely, thank you. Able to see the traffic from the target, only thing is that after running for a little while, it starts to say "arp.spoof could not find spoof targets". I think it is my network adapter that fails or the internet on the attacking machine.

----- Edit2

Apparently net.probe can conflict with arp spoofing, so turn it off before continuing with the mitm. In case anyone has the same problem

pomwtin - February 12, 2023, 7:38 am

If you are up for a challenge you can try to expire certificates using delorean or cacheraser. Depending on targeted OS, the attack can be purely technical or client-side.

After certificate expiration you can effectively use SSL-strip, with exception of webpages which does not allow traffic on plain http

am0rph0us - March 8, 2023, 6:47 pm

(Feb 12, 2023 08:38 AM)pomwtin Wrote: [\[CITE\]](#) If you are up for a challenge you can try to expire certificates using delorean or cacheraser. Depending on targeted OS, the attack can be purely technical or client-side.

After certificate expiration you can effectively use SSL-strip, with exception of webpages which does not allow traffic on plain http

Really good suggestions, delorean sounds cool. These attacks are also from around 2015 are they still viable or mostly patched?

Also, do you have an open source copy of CachEraser? Want to try it

SIM-5330817 - March 10, 2023, 10:33 pm

